¿Se puede evitar el próximo Wikileaks?

1 de mayo

2011

Mucho se ha hablado del “fenómeno” Wikileaks y de lo que ello representa(rá) para el presente y el futuro de la información, la libertad de expresión y la seguridad nacional y corporativa. El objetivo del presente es plantear una serie de preguntas para abrir el debate entre los profesionales de seguridad, el derecho, los medios no especializados, los gobiernos, las empresas y el público en general, sobre la fuga de información

Autor: Lic. Cristian Borghello CISSP-MVP

Versión: 1.1 (20110501)

Descarga: www.segu-info.com.ar

Artículo originalmente publicado como nota de tapa en la Revista CXO 13: http://cxo-community.com/revista-impresa/3898.html

¿Problemas nuevos?

Ya, en 1971 "**los papeles del Pentágono"** representaron la mayor fuga de información y escándalo, al ser revelado un "informe secreto" del Departamento de Defensa (DoD) de EE.UU. sobre su invasión militar y política a Vietnam entre 1945 y 1967. Cuarenta años después, nuevamente se discuten los mismos temas al ser revelados los 250 mil documentos del caso Wikileaks [1].

En 2006, la cantidad de información digital creada, capturada y replicada fue mayor que la generada en los 5.000 años anteriores y entre 2009 y 2020 esta cantidad crecerá en un factor de 44 veces. [EMC]

No hay nada para agregar a la inteligencia internacional y al espionaje industrial que ya no se haya dicho antes. El robo de datos por parte de atacantes internos (*insiders*) es el motivo más antiguo de fuga de información confidencial desde que el mundo es mundo y, esta fuga, no hizo más que facilitarse y potenciarse con la masificación de los medios digitales, que permiten su duplicación y distribución en forma casi instantánea.

Por eso son necesarias las medidas de seguridad internas que toda organización debería tomar con sus empleados, ya que son estos los que tienen el poder de obtener y robar información confidencial, ante la más mínima "provocación" como puede ser un disgusto con la organización o sus directivos, un motivo político o simplemente la "infalible" tentación monetaria.

¿El hombre prudente existe?

Quizás lo que realmente se esté discutiendo de fondo, cuando se dejan de lado las banalidades que se mencionan en el caso de Wikileaks, es el tratamiento que los gobiernos y las corporaciones deben dar a la información y cómo este tratamiento debe estar regido por el **principio del hombre prudente**: la responsabilidad y el cuidado debido y razonable (*dure care* y *dure diligence*) de la información requieren que los responsables de cualquier organización pública o privada realicen sus acciones con diligencia y cuidado… tal y como lo haría cualquier hombre prudente o de familia.

¿Héroes, delincuentes o mercaderes de la información y el poder?

Es imposible siquiera rascar la superficie de un complicado entramado internacional que envuelve a un hacker (Julian Assange así lo demuestra siendo co-autor del libro "*Underground: Tales of hacking, madness and obsession on the electronic frontier*" de finales de los '80 [2]), gobiernos y poderes políticos de varias potencias mundiales, personajes millonarios que brindan su soporte desde las sombras, grupos económicos acusados de estafas y fraudes, empresas de seguridad privadas que realizan espionaje para gobiernos [3], periodistas, activistas y grupos de usuarios *"Anonymous"* [4] que se auto-erigen como héroes de los usuarios de Internet y realizan delitos y ataques informáticos a diestra y siniestra, en nombre de la libertad de expresión.

Lo que sí queda claro es que la información y su fuga representan un gran negocio para muchas organizaciones y mientras las compañías siguen evaluando si es conveniente capacitar a los usuarios o instalar tal o cual producto, la discusión pasa por otros lares: existen intereses creados que tienen muy en claro que quien disponga de la información y de la capacidad de ataque de las redes distribuidas, tendrá el poder de los próximos años.

Espionaje digital y ciberguerra ¿qué sigue?

Ataques de denegación de servicios distribuidos (DDoS) como los recientemente realizados por el grupo *Anonymous* a empresas como VISA, Mastercard y a organizaciones de derechos de autor e incluso religiosas, demuestran el poder político, de militancia, reclamo y protesta que miles de usuarios pueden ejercer en la red, utilizando incluso herramientas dañinas y cometiendo delitos. Ese hecho también queda manifiesto en la importancia que adquirió Internet en los conflictos civiles de Túnez y Egipto.

> *El 85% de las organizaciones han sufrido fugas de información por parte de sus empleados, clientes o proveedores en los últimos dos años.* [Ponemon Institute]

Por otro lado, el robo de información y ataques cibernéticos explícitos como Operación Aurora [5] desde China y hacia Google, Adobe, Intel y otras treintena de empresas y el gusano Stuxnet [6] contra el gobierno iraní y sus instalaciones nucleares, confirman que la ciberguerra ha comenzado hace tiempo y que los gobiernos no dudarán en utilizar su potencial tecnológico para tomar ventaja bélica.

No hay conclusiones, sólo más preguntas

Basándose en el principio del hombre prudente, las organizaciones y los gobiernos deben comprender que no podrán reclamar indemnizaciones o reconocimientos si no han protegido sus activos en forma consistentes con la confidencialidad e importancia de los mismos, han asumido un riesgo excesivo o han procedido con negligencia.

En lo que respecta a los gobiernos, es hora que los países latinoaméricanos y sus soberanos despierten y se den cuenta que el Siglo XXI comenzó hace tiempo y que la información apunta a ser el nuevo “arma de destrucción masiva” y por lo tanto, debe usarse pero sobre todo protegerse.

Volviendo a la pregunta inicial es casi seguro que no se puede evitar un próximo Wikileaks, o como se llame, pero eso no significa que no se deba estar preparado para lidiar con él. En resumen, la sociedad de hoy debe *“regresar a lo antiguo, volver a eso que fue bueno”* -Aristóteles dixit - porque Wikileaks y sus sucesores ha producido un quiebre en la forma de tratar la información y la libertad de expresión de las próximas generaciones.

¿Cómo evitar fuga de información?

- A continuación se detalla algunos procedimientos, controles y herramientas que pueden ser utilizados para evitar o dificultar la fuga de información confidencial desde las organizaciones:
- Clasificar la información: establecer los niveles de criticidad así como la prioridad en su protección.
- Mínimo Privilegio: limitar a los usuarios a acceder sólo a los recursos necesarios para ejecutar sus tareas.
- Separación de tareas: asegurar que un individuo no puede realizar tareas completas por sí mismo.
- Conocimiento distribuido y control dual: se requieren dos o más individuos para realizar una tarea.
- Control de cambios: registrar cada cambio de cada documento (responsable, motivo, fecha, versión, etc.).
- Autenticación fuerte: utilizar dos o más factores de autenticación para asegurar que un usuario es quien dice ser.
- Metadatos: todos los tipos de archivos (imágenes, documentos, etc.) deben ser verificados para eliminar datos que puedan brindar información propia del archivo (datos de red, autores, nombres de usuarios, fechas, nombre de impresoras, etc.).
- Marcas de agua: en ciertos tipos de documentos puede ser recomendable utilizar texto, imágenes o audio que aparezcan detrás o encima del documento impreso o digital. Su existencia puede facilitar la identificación y autenticación del documento y dificultar su copia o duplicación
- Cifrado de la información: toda la información debe cifrarse con métodos reconocidos por la industria y que cumplen los estándares internacionales. El cifrado debe realizarse sobre la información que almacenada y cuando se transmite.
- Firmado digital (o electrónico) de documentos: proceso que mediante el uso de la criptografía permite identificar y autenticar mensajes o documentos.
- Data Loss Prevention (DLP): aplicaciones que permiten el monitoreo y control de los datos digitales en una infraestructura tecnológica.
- Logs: el proceso de autorización tiene como objetivo que cada usuario, tarea y fecha sea identificado y rastreable (pistas de auditoría)
- Backup: las copias de seguridad y su recuperación efectiva y eficiente son la única solución cuando todo lo demás ha fallado.
- Nota: el almacenamiento en la nube no cambia nada de lo anterior y se debe procurar que los contratos de servicios (SLA) así lo establezcan con el proveedor.

Referencias

[1] Wikileaks
http://www.segu-info.com.ar/wikileaks/

[2] *Underground: Tales of hacking, madness and obsession on the electronic frontier.* Dreyfuss, Assange
http://bit.ly/iff7EY
http://amzn.to/dXj2aZ

[3] Conspiración del Departamento de Justicia de EEUU y el Bank of America para silenciar a Wikileaks y periodistas
http://bit.ly/elBSLU

[4] Información sobre Anonymous
http://bit.ly/segu-anonymous

[5] Operación Aurora
http://blog.segu-info.com.ar/2010/12/faq-sobre-stuxnet.html

[6] Stuxnet
http://blog.segu-info.com.ar/2010/12/faq-sobre-stuxnet.html